2009 Fifth International Conference on Autonomic and Autonomous Systems

Survey on Security Challenges for Swarm Robotics

Fiona Higgins, Allan Tomlinson and Keith M. Martin
Information Security Group, Royal Holloway, University of London
Egham Hill, Egham. Surrey. TW20 0EX. U.K.
f.l.higgins, allan.tomlinson, keith.martin@rhul.ac.uk

Abstract

Swarm robotics is a relatively new technology that is being explored for its potential use in a variety of different applications and environments. Previous emerging technologies have often overlooked security until later developmental stages, when it has had to be undesirably (and sometimes expensively) retrofitted. We identify a number of security challenges for swarm robotics and argue that now is the right time to address these issues and seek solutions. We also identify several idiosyncrasies of swarm robotics that present some unique security challenges. In particular, swarms of robots potentially (i) employ different types of communication channels (ii) have special concepts of identity, and (iii) exhibit adaptive emergent behaviour which could be modified by an intruder. Addressing these issues now will prevent undesirable consequences for many applications of this type of technology.

Keywords: swarm robotics, security, autonomy, adaption, emergent behaviour.

1. Introduction

Swarm robotics is a relatively young area of research, which is growing rapidly and comprehensive reviews of the state-of-the-art may be found in [1, 2, 4]. As with many technologies, there is no formal definition for swarm robotics that engenders universal agreement, however there are some characteristics that have been generally accepted. These include robot autonomy; decentralised control; large numbers of member robots; collective emergent behaviour and local sensing and communication capabilities. From our security perspective it is reasonable to consider swarm robotics as a special type of computer network with the aforementioned characteristics.

It has often been the case that the security of a new technology is an afterthought rather than an upfront design objective, leading to many security issues. This was the case with, for example, mobile phone technology. The first generation of mobile phones were analogue, and easy to clone since they broadcast their identity clearly over the airwaves. It was also easy to eavesdrop on them by simply tuning a radio receiver to pick up conversations. Subsequently the underlying technology had to be expensively modified in order to address these threats. In the case of swarm robotics research, the particular security requirements of swarm robotic networks do not appear to have been investigated in any detail so far. Thus we believe that this is an opportune time to consider these issues, before any wide-scale deployment. Deferring security research until later in the technology's evolution could, depending on the application, be a risky strategy and lead to undesirable consequences.

As far as we are aware, this is the first attempt to categorise security challenges to swarm robotics. Very little prior work appears to have been done. A notable exception to this is the work of Winfield and Nembrini [29] who identify several threats to a swarm of robots, which they classify as hazards. We hope that our identification of the main security challenges will result in the development of robot swarm technology that is reliable and safe to deploy even in potentially hostile environments.

In Section 2 we briefly review technologies that are similar to swarm robotics, highlighting the key differences. In Section 3 we discuss security, commencing with a short high level overview of security, and then cataloguing aspects of the swarm robotic environment which present challenges to security. In Section 4 we provide examples of applications where swarm robotics could be used. Finally in Section 5 we draw some conclusions.

2. Related Technologies

Before considering the security of swarm robotic networks it will be useful to review how similar technologies,

978-0-7695-3584-5/09 $25.00 © 2009 IEEE
DOI 10.1109/ICAS.2009.62

some of which have been subjected to a degree of security analysis, relate to robotic swarms. This will allow us to identify the unique features of robotic swarms that may benefit from closer scrutiny in terms of security.

2.1. Multi-Robot Systems

Swarm robotics differs from more traditional multi-robot systems in that their command and control structures are not hierarchical or centralised, but are fully distributed, self-organised and 'inspired by the collective behaviour of social insect colonies and other animal societies' [5]. Self-organisation means that sometimes the collective behaviour, even if unpredictable, may well result in solutions to problems that are superior to ones that could have been devised in advance. The parallel drawn with social societies in the animal world extends to communication – interactions between the robots can be indirect as well as direct. *Fault-tolerance*, which is related to security, has already been extensively researched within the context of multi-robot systems with hierarchical command and control, notably in the work of Parker's ALLIANCE control architecture [20].

2.2. Mobile Sensor Networks

Sensor networks consist of collections of devices (or *nodes*) with sensors that typically communicate over a wireless network. A *mobile* sensor network is a sensor network where the nodes are either placed on objects which move [27] or where the nodes may move themselves [9]. In the latter case they are sometimes known as *robotic sensor networks* [18]. Hybrid systems also exist [21], where mobile robots work in conjunction with static sensors. Although mobile sensor networks exhibit many similarities to swarm robotic networks, there are distinct differences. For example, robotic swarms may utilise a wider range of communications technologies, which extend to indirect communication such as stigmergy. Stigmergy is discussed further in Section 3.2. Additionally, individual identity may be more important in a sensor network if it is important to determine exactly where some sensed data originated. Furthermore, and importantly, a sensor network is not designed to have the collective emergent behaviour of a robotic swarm.

2.3. MANETs

Mobile Ad-hoc Networks *(*MANETs*)* consist of wireless mobile nodes that relay each others' traffic, with the nodes spontaneously forming the wireless network themselves. The special properties of MANETs, such as the lack of infrastructure, absence of trusted third parties, as well as possible resource constraints, make implementing security a very challenging task. MANETs can consists of many types of mobile devices and there is considerable existing work on their security [7, 17]. Although MANETs do not exhibit the emergent behaviour of swarms, some MANET security techniques could have relevance to swarm robotics depending on the communication method used by the swarm.

2.4. Software Agents

There is no universally agreed definition of a software agent, but we take one proposed by Wooldridge [30]: 'An *agent* is a computer system that is situated in some environment, and that is capable of autonomous action in this environment in order to meet its design objectives'. A *multi-agent system* (MAS) [6, 30] is a system composed of multiple autonomous agents, where each agent cannot solve a problem unaided; there is no global system control; data is decentralised; and computation is asynchronous. A *mobile* agent is a particular class of agent with the ability during execution to migrate from one host to another where it can resume its execution [6]. Thus *mobile multi-agent systems* may share many features with swarm robotic systems, but in a virtual world.

Corresponding to the active interest in mobile software agents and their rapid adoption, there has been much interest in their security [6]. However this does not always translate easily to robotic swarms because of the particular characteristics of robotic swarms which differentiate them, such as their physical nature, diverse communication mechanisms and control structure.

3. Security of Swarm Robotics

3.1. Basic Security Terminology

Security in any environment, including swarm robotics, is fundamentally about the provision of core *security services*, some of the most important of which are as follows. The service *confidentiality* is about keeping data secret. An *integrity* service prevents prevents data from being altered in an unauthorised or unintended way. *Entity authentication* (sometimes called *identification*) is the process whereby one entity is assured of the identity of another entity. *Data origin authentication* is the assurance that data came from its reputed source. Finally, *availability* is the property of being accessible and useable upon demand by an authorised entity. The term *denial of service* is often used in reference to loss of availability.

A *threat* is a potential violation of the provision of a desired security service. Threats that are not mitigated leave *vulnerabilities* in the system that may be exploited. Such exploitative actions are often called *attacks* and those that initiate their execution are *attackers*. An example of a threat

could be that an unauthorized person might see top secret information; a vulnerability could be that trust is misplaced in a courier; an attack could be that someone steals the data and publishes it in the media. Information may also be *accidentally* lost. The impact of a document theft or loss will depend on the content of the document. The process of *risk assessment* takes this into consideration along with the probability of the threat being realised.

In any system, the provision of security is a holistic process. This requires careful management processes that oversee the use of specific security technologies that can be applied to devices and networks. These include *firewalls*, *access control mechanisms* and *network security protocols*. At the heart of most security technologies is the deployment of specific *cryptographic primitives*, which are mathematical tools that can be applied to data to provide the core security services. These normally rely on the careful protection and maintenance of *cryptographic keys*, which are critical data items that must be stored securely.

3.2. Challenges to Security in a Swarm Robotic Environment

It is appropriate therefore to consider the challenges to providing security in swarm robotic networks. It is clear that some security issues are similar to other related technologies and that some solutions from these technologies may apply to swarm robotics. However, not all of these shared problems have been fully solved. Furthermore, the swarm robotic environment introduces particular security challenges that do not exist in other technologies.

Resource Constraints: The smaller a device is, the greater the challenge to providing security due to resource constraints (storage, communication bandwidth, computational restrictions and most importantly energy). Attacks on the provision of resources can lead to the device becoming inoperable, permanently so if the resource is not renewable. This leads to a loss of availability. Resource constraints also restrict the types of existing security technologies that can be deployed.

Physical Capture and Tampering: Physical capture of a robot leads to loss of availability. Worse, capture of security credentials could harm other members of the swarm. If a robot is tampered with and reintroduced into the swarm, an attacker might influence the swarm behaviour. This attack would be unique to swarm robotic technology.

Control: Systems employing swarm intelligence do not have a hierarchical structure with points of control. The individuals within these systems take decisions autonomously, based on local sensing and communications. With such systems it is evident that there could be many risks if they went 'out-of-control', including many security violations such as loss of confidentiality or availability. Control presents an interesting challenge to security within swarm robotics.

Communication: Swarm robots can interact either explicitly, or implicitly [19]. *Explicit* communication can be achieved via broadcast or directed messages. Radio-frequency (RF) and infra-red (IR) technologies have been widely for explicit communications within swarms. Other technologies include coloured LED display, body-language or sign-language, colour patterns on a robot's body, coil induction, haptics, audible sounding, combination of LED display and audio signalling and acoustic signalling in an underwater environment. *Implicit* communication includes interaction via sensing other robots and their behaviours, and interaction via the environment, which acts as a sort of shared memory and is known as *stigmergy* [5, 16, 28].

From a security perspective, any open implicit or explicit communication method can be jammed, intercepted or otherwise disturbed relatively easily by an attacker. The security of RF and IR has been well researched but the security of the remaining more 'exotic' interaction methods needs to be thoroughly investigated and presents a fascinating security challenge.

Swarm Mobility: Security is difficult to provide in any mobile environment, however the mobility of robot swarms is quite unusual and has some interesting characteristics that might make some security services easier to implement than for related technologies. One example is entity authentication, discussed below, which could be provided through visual sensing and physical data exchange. However any constraint on the movement of swarm members, for example to remain in the 'bounds' of the swarm could present additional security issues.

Identity and Authentication: As discussed in Section 4, it may be very important for a swarm robot to determine if it is interacting with a legitimate entity or not. Data origin and entity authentication require some notion of *identity*, which is a particular problem where *individual identity* within a swarm is undesirable [13]. Other work has used *group identity* [22]; or individual identity which is broadcast regularly [14]. If identity can be assumed or changed then attacks can be launched on entity authentication, confidentiality, integrity and availability. The notion of identity within a robotic swarm thus presents an interesting challenge from a security standpoint.

Key Management: Security services deployed in a robot swarm inevitably require the need to manage cryptographic keys [10]. These keys define which pairs (or groups) of robots can apply security services. As robots join and leave a swarm, it may be necessary to alter this keying material. Thus the dynamic and interactive nature of a swarm presents sophisticated key management challenges.

Intrusion Detection: When a foreign entity joins a network it is sometimes called *intrusion*. One means of de-

tecting intrusion is based on network *Intrusion Detection Systems*. The autonomous nature of robots and collective emergent nature of the behaviour of the swarm will make any anomalous behaviour difficult to detect. If undetected, one or more foreign robots could infiltrate the swarm, either maliciously or accidentally, and ultimately affect the desired emergent behaviour.

Once an intruder is detected, an appropriate response will need to be formulated according to an *Intrusion Protection System*. Depending on the application the response could be to simply ignore the rogue device, or to monitor its behaviour, or to find a way to either disable it or remove it from the system. Intrusion detection and protection looks to be particularly challenging in a swarm of robots, and will need a specifically tailored approach.

Managing Learning: Robots can learn and react to environmental changes by means of adaption. A malicious entity might present changes in the environment which will cause a robot to adapt in an undesired way. For example, if anomaly detection is used to detect intrusion based on learning typical behaviour, then a malicious entity could change the pattern of 'typical' behaviour in order to gain entry to the network.

4. Examples of Use for Swarm Robotics

Mass production of low-cost robots is essential for the viable deployment of swarm robotic systems. Rapid advances in mechatronics technology, as well as other new innovations are already making the construction of smaller and cheaper robots possible. In this section we will discuss some potential applications for swarm robotics.

4.1 Military

Swarm robotic networks may be used in military applications where the need for security is perhaps self-evident. There is currently much research taking place in this area. In the United Kingdon in August 2008, a challenge called 'The Grand Challenge' [26] took place, which was searching for the best ideas in defence technology to help solve some of the evolving threats facing front line troops. One prominent entrant to this was 'Swarm Systems'[24], which used swarms of micro air vehicles.

In the United States, US Army Research are funding and working with BAE Systems on the The Micro Autonomous Systems and Technology (MAST) project [3] which will "research and develop advanced robotic equipment for use in urban environments and complex terrain, such as mountains and caves. The project will create an autonomous, multifunctional collection of miniature intelligence-gathering robots that can operate in places too inaccessible or dangerous for humans".

4.2 Monitoring

Robot swarms are well suited to monitoring and potentially could provide solutions in the case of undesired events. For example, the Elimination Units for Marine Oil Pollution (EU-MOP) project demonstrated that they could be used to detect environmental pollutants such as oil spillages, and clean them up [15].

At the Ecole Polytechnique Federale de Lausanne (EPFL) they have investigated how swarm robotics could be used for the autonomous inspection of complex engineered structures [8].

In addition to malfunctions or accidents, there could be threats to such robot swarms from parties such as terrorists or criminals. Such groups could target the availability of the swarms, or the confidentiality or integrity of any information that they hold. For example they could physically or electronically hijack robots leading to loss of availability. They could potentially use such a situation to extort money from the legitimate owners of the swarm, with the robots only being returned to use after a ransom has been paid. Many such attacks have already been launched against business websites on the internet.

The data that a swarm holds could be useful to a non-legitimate third party. For example the location and extent of an oil spillage could be of great worth to an environmental group; the location of faults in a structure could be of great interest to a competitor. Therefore, it is of importance that such data is kept confidential. Also, if such data could be corrupted accidentally or deliberately, it could lead to the swarm performing incorrectly, which could mean that monitoring is not taking place properly or the swarm is not trying to fix something that it is meant to be.

4.3 Disaster Relief

Robot swarms could be deployed during disaster relief operations. For example the European Union 6th Framework GUARDIANS project [11] utilises a swarm of autonomous robots to navigate and search in situations which are dangerous and time-consuming for humans thus enhancing operational safety and saving lives. The robots also warn of toxic chemicals, and provide and maintain mobile communications links. At the University of Utah, research has taken place into using swarms of robots to aid first responders in disaster situations [23].

In situations such as these, availability becomes a primary security requirement, as well as confidentiality, integrity and authentication/identification. Availability is necessary so that the swarm can respond as quickly as possible to the emergency at hand. If robots are unavailable due to malfunction, accident or because they have been hijacked either physically or electronically by an external

agency, then they will be unable to perform their critical task. Confidentiality could be necessary to safeguard information about entities that the robots come across, such information could be highly sensitive or of other interest to malicious parties. Integrity is necessary to ensure that the data being passed around the swarm is accurate, so that the robots respond correctly. Authentication/identification is necessary to ensure that sensitive information is communicated only to legitimate parties, and to members of the correct swarm if multiple swarms are in joint operation.

Many relevant current technologies already provide full support for strong security. Communications between human personnel in emergency situations often use Terrestrial Trunked Radio (TETRA) [25] which is an open digital standard defined by the European Telecommunications Standard Institute (ETSI).

4.4 Healthcare

The use of swarm robotics has been considered for a wide range of healthcare services, from surgery and intra-body diagnostics to more routine tasks such as medication provision and patient monitoring. The European I-Ward project uses swarms of robots to provide assistance to healthcare workers [12].

Entity authentication will be very important for swarm robotics in healthcare situations. For example, it will be of vital importance that only legitimate robots are introduced into a human body, or sent to deliver patient medicines or read patient data from monitoring stations. If this were not the case then malicious third parties could attack individuals by introducing swarm robots that would harm the patient surgically or whilst inside their body, by delivering incorrect medicines or by stealing their data.

The confidentiality or privacy of patient data is also paramount, and is protected by law in many countries. Apart from patients wanting to be able to choose who knows their personal medical history, it must be kept from organisations who may wish to have it for reasons such as drug research or to simply try and deny an individual access to insurance, employment or services. Integrity of medical information must be ensured, otherwise a swarm could damage a patient by responding to incorrect information such as wrong organ position, elevated blood pressure or blood sugar levels. To respond incorrectly could seriously damage the patient's health, maybe fatally. Availability of swarm robots in a healthcare situation is important, especially so where they are deployed in situations with critically ill patients. If they are not available and able to respond immediately then such patients could suffer greatly, and maybe die as a result.

4.5 Commercial Applications

As the technology develops, robotic swarms will find commercial use. Commercial uses could include applications already discussed, for example monitoring or healthcare, as well as many others.

In any commercial application the motivation to interrupt, steal or amend data and services by ill-intentioned competitors will lead to threats to confidentiality, integrity and availability. For example if an organisation can interrupt their competitors service and make it unavailable or unstable, damaging its reputation, then they will become the organisation of choice. If they can steal information from their competitor then they may be able to find out their trade secrets for their own commercial gain. If they can amend their competitors data then they can make them operate unpredictably, again damaging their reputation, and making themselves appear preferable.

For commercial applications to be successfully deployed, consideration must be given beforehand to the potential security risks.

5. Conclusions

As discussed in the previous section, the development of swarm robotic technology has reached a point where many new applications are emerging. Therefore, we believe that this is an opportune moment to take a closer look at the security of swarm robotic systems - before widespread deployment. Although the security of related technology has been investigated, robotic swarms are different due to factors such as their autonomy, distributed control, and emergent behaviour. Bearing this in mind, we have identified a number of significant challenges to robotic swarm security, some of which are unique to this technology. For example, the challenges presented by more esoteric communication methods than straightforward RF or IR, the question of identity, and the potential for modification of emergent behaviour if a malicious entity manages to infiltrate the swarm. It is likely that some of these challenges will require new security techniques to be developed, and we will aim to investigate these in our future work.

References

[1] E. Şahin and W. Spears, editors. *Swarm Robotics Workshop: State-of-the-art Survey*, volume 3342 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin Heidelberg, 2005.

[2] E. Şahin, W. Spears, and A. Winfield, editors. *Swarm Robotics. Revised Selected Papers from the Second International Workshop, SAB 2006. Rome. Italy.*, volume 4433/2007. Springer Berlin/Heidelberg, 2007.

[3] BAE-Systems. Mast project. http://www.baesystems.com, April 2008.

[4] L. Bayindir and E. Şahin. A review of studies in swarm robotics. *Turkish Journal of Electrical Engineering*, 15:115–147, 2007.

[5] E. Bonabeau, M. Dorigo, and G. Theraulaz. *Swarm Intelligence: from natural to artificial systems (Santa Fe Institute Studies in the Sciences of Complexity).* Oxford University Press, 1999.

[6] N. Borselius. *Multi-agent system security for mobile communication*. PhD thesis, Department of Mathematics, Royal Holloway, University of London., 2003.

[7] L. Buttyán and J.-P. Hubaux. *Security and Cooperation in Wireless Networks: thwarting malicious and selfish behaviour in the age of ubiquitous computing*. Cambridge University Press, 2007.

[8] N. Correll and A. Martinoli. A challenging application in swarm robotics: The autonomous inspection of complex engineered structures. *Bulletin of the Swiss Society for Automatic Control*, 46:15–19, 2007.

[9] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. Sukhatme. Robomote: Enabling mobility in sensor networks. In *Proceedings of Fourth International Symposium on Information Processing in Sensor Networks*, pages 404–409, 2005.

[10] S. Dolev, L. Lahiani, and M. Yung. Secret swarm unit. reactive k-secret sharing. In *Proc. of the 8th International Conference on Cryptology in India*, pages 123–137. Springer Verlag, 2007.

[11] EU. European union 6th framework programme: Guardians project. http://www.guardians-project.eu/, 2007.

[12] EU. European union 6th framework programme: Iward: Intelligent robot swarm for attendance, recognition, cleaning and delivery. http://www.iward.eu/, 2007.

[13] P. Flocchini, G. Prencipe, N. Santoro, and P. Widmayer. Gathering of asynchronous robots with limited visibility. *Theoretical Computer Science*, 337(1-3):147–168, 2005.

[14] J. Fredslund and M. Matarić. A general algorithm for robot formations using local sensing and minimal communication. *IEEE Transactions on Robotics and Automation*, 18:837–846, 2002.

[15] K. Gkonis, T. Pavlidis, N. Kakalis, and N. Ventikos. Final project report for the elimination units for marine oil pollution (eu-mop) project. Technical report, European Union, 6th Framework Programme, 2008.

[16] P.-P. Grassé. La reconstruction du nid et les coordinations inter-individuelles chez bellicositermes natalensis et cubitermes sp. la théorie de la stigmergie: Essai d'interprétation du comportement des termites constructeurs. *Insec. Soc.*, 6:41–80, 1959.

[17] E. Hansson, A. Bengtsson, and A. Vidström. Security solutions for mobile ad hoc networks. Technical Report FOI-R–1694–SE ISSN 1650-1942, Swedish MOD, FOI Defence Research Agency Command and Control Systems P.O. Fox 1165 SE-581 11 Linköping Tel 013-378086, August 2005.

[18] MinnesotaUniversity. Robotic sensor networks. http://rsn.cs.umn.edu, 2008.

[19] L. Parker. Current state of the art in distributed autonomous mobile robotics. *Distributed Autonomous Robotic Systems*, 4:3–12, 2000.

[20] L. E. Parker. ALLIANCE: An architecture for fault tolerant multi-robot cooperation. *IEEE Transactions on Robotics and Automation*, 14(2):220–240, April 1998.

[21] J. Reich and E. Sklar. Toward automatic reconfiguration of robot-sensor networks for urban search and rescue. In *Proceedings of the 1st International Workshop on Agent Technology for Disaster Management*, 2006.

[22] R. A. Russell. Visual recognition of conspecifics by swarm robots. In *2004 Australasian Conference on Robotics & Automation*, 2004.

[23] D. Stormont. Autonomous rescue robot swarms for first responders. In *CIHSPS 2005 - IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety Orlando FL USA, 31 March - 1 April 2005*, 2005.

[24] Swarm-Systems. Swarm systems: providing swarms of micro air vehicles. http://www.swarmsys.com, August 2008.

[25] Tetra-Association. Terrestrial trunked radio. http://www.tetra-association.com/, 2008.

[26] UK-MOD. United kingdom ministry of defence: The grand challenge. http://www.challenge.mod.uk, August 2008.

[27] T. Wark, C. Crossman, W. Hu, Y. Guo, P. Valencia, P. Sikka, P. Corke, C. Lee, J. Henshall, K. Prayaga, J. O'Grady, M. Reed, and A. Fisher. The design and evaluation of a mobile sensor/actuator network for autonomous animal control. In *Proceedings of the 6th international conference on Information processing in sensor networks*, pages 206–215. ACM, 2007.

[28] T. White. Expert assessment of stigmergy: A report for the department of national defence. Technical report, School of Computer Science, Carleton University, Ottawa, Ontario, Canada, 2005.

[29] A. Winfield and J. Nembrini. Safety in numbers: fault-tolerance in robot swarms. *International Journal of Modelling, Identification and Control*, 1:30–37, 2006.

[30] M. Wooldridge. *An Introduction to MultiAgent Systems*. Wiley, 2002.